A Class of Permutation Polynomials of $\mathbf{F}_{2^m}$ Related to Dickson Polynomials

Henk D. L. Hollmann
Philips Research Laboratories
Prof. Holstlaan 4, 5656 AA Eindhoven
The Netherlands
email: henk.d.l.hollmann@philips.com

Qing Xiang
Department of Mathematical Sciences
University of Delaware
Newark, DE 19716, USA
email: xiang@math.udel.edu

February 1, 2008

Abstract

We construct a class of permutation polynomials of $\mathbf{F}_{2^m}$ that are closely related to Dickson polynomials.

1 Introduction

Let $\mathbf{F}_q$ be a finite field of order q, where q is a prime power. We write $\mathbf{F}_q \setminus \{0\}$ as $\mathbf{F}_q^*$. A polynomial $f(X) \in \mathbf{F}_q[X]$ is called a *permutation polynomial* (PP) of $\mathbf{F}_q$ if the associated polynomial function $f : c \mapsto f(c)$ from $\mathbf{F}_q$ to itself is a permutation of $\mathbf{F}_q$. Permutation polynomials have been studied extensively in the literature, see [6], [7], [8], [11] for surveys of known results on PPs. A very important class of polynomials whose permutation behavior is well understood is the class of Dickson polynomials, which we will define below.

Let $a \in \mathbf{F}_q$ and let n be a positive integer. We define the *Dickson polynomial* $D_n(X, a)$ over $\mathbf{F}_q$ by

$$D_n(X, a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j X^{n-2j},$$

where $\lfloor n/2 \rfloor$ is the largest integer $\leq n/2$. Alternatively we may define the Dickson polynomial $D_n(X, a)$ to be the unique polynomial of degree n over $\mathbf{F}_q$ such that

$$D_n(X + \frac{a}{X}, a) = X^n + \left(\frac{a}{X}\right)^n. \tag{1}$$

We refer the reader to [9, p. 8–9] for explanations on why (1) can be used to define the Dickson polynomials. The PPs among the Dickson polynomials have been completely classified. We state the following theorem due to Nöbauer [10].

Theorem 1.1 *The Dickson polynomial $D_n(X, a)$, $a \in \mathbf{F}_q^*$, is a permutation polynomial of $\mathbf{F}_q$ if and only if* $\gcd(n, q^2 - 1) = 1$.

A proof of this theorem can be found in the original paper of Nöbauer [10] or in [6, p. 356]. Dickson in his 1896 Ph. D. thesis observed and partially proved the theorem.

In this note, we construct a family of permutation polynomials of $\mathbf{F}_{2^m}$. These polynomials are closely related to Dickson polynomials $D_n(X, 1)$ over $\mathbf{F}_{2^m}$, where n is of the form $2^k - 1$. (See Proposition 2.3 for the relation.) We state our main results as follows.

Let $m \geq 1$ be an integer, let k be an integer in $\{1, \ldots, m-1\}$ with $\gcd(k, m) = 1$, and let $r \in \{1, \ldots, m-1\}$ be such that $kr \equiv 1 \bmod m$. Define the integer m' by $kr = 1 + mm'$ and write $q = 2^m$ and $\sigma = 2^k$. Throughout the rest of the note, we will keep the definitions of m, k, r, m', q, σ fixed. We will use Tr to denote the trace from $\mathbf{F}_q$ to $\mathbf{F}_2$ and for $e \in \mathbf{F}_2$ we set

$$\mathbf{T}_e = \{x \in \mathbf{F}_q \mid \mathrm{Tr}(x) = e\}.$$

Also we define $\mathrm{Tr}(X)$ to be the following polynomial in $\mathbf{F}_2[X]$.

$$\mathrm{Tr}(X) := X + X^2 + \cdots + X^{2^{m-1}}.$$

For α, γ in $\{0, 1\}$, we define the polynomials

$$H_{\alpha,\gamma}(X) := \gamma \mathrm{Tr}(X) + \frac{\left(\alpha \mathrm{Tr}(X) + \sum_{i=0}^{r-1} X^{\sigma^i}\right)^{\sigma+1}}{X^2}.$$

(Note that $H_{\alpha,\gamma}(X)$ is indeed a polynomial in X with coefficients in $\mathbf{F}_2$ and $H_{\alpha,\gamma}(0) = 0$.)

Our main theorem is

Theorem 1.2 *Let m, k be positive integers with $\gcd(k, m) = 1$, let $r \in \{1, \ldots, m-1\}$ be such that $kr \equiv 1 \pmod{m}$, and let $\alpha, \gamma \in \{0, 1\}$. Then the mapping $H_{\alpha,\gamma} : x \mapsto H_{\alpha,\gamma}(x)$, $x \in \mathbf{F}_q$, maps $\mathbf{T}_0$ bijectively to $\mathbf{T}_0$, and maps $\mathbf{T}_1$ bijectively to $\mathbf{T}_{r+(\alpha+\gamma)m}$. In particular, the polynomial $H_{\alpha,\gamma}(X)$ is a PP of $\mathbf{F}_{2^m}$ if and only if $r + (\alpha + \gamma)m \equiv 1 \pmod{2}$.*

The polynomials $H_{\alpha,\gamma}(X)$ arose in our recent work on the association scheme afforded by the action of $\mathrm{PGL}(2, q)$ on the set of exterior lines to a non-degenerate conic in $\mathrm{PG}(2, 2^m)$ [4]. In order to prove that the fusion by the Frobenius map of the aforementioned association scheme is pseudocyclic, we need to investigate the permutation behavior of the polynomials $H_{\alpha,\gamma}(X)$. We believe that the polynomials $H_{\alpha,\gamma}(X)$ are of independent interest. In Section 2, we will explain the connection between Dickson polynomials and the polynomials $H_{\alpha,\gamma}(X)$. In Section 3, we give a proof of our main theorem.

2 Relating $H_{\alpha,\gamma}(X)$ to Dickson Polynomials

Let m, k, r, m', q, σ be defined as in Section 1, so that $\gcd(k, m) = 1$ and $kr = 1 + m'm$. For $\alpha, \beta \in \{0, 1\}$, we define the polynomials

$$f_\alpha(X) := \alpha \mathrm{Tr}(X) + \sum_{i=0}^{r-1} X^{\sigma^i},$$

and

$$g_\beta(X) := \beta \mathrm{Tr}(X) + \sum_{j=0}^{k-1} X^{2^j}.$$

We will use f_α and g_β to denote the associated polynomial functions from $\mathbf{F}_q$ to $\mathbf{F}_q$. Also using $f_\alpha(X)$, we can rewrite $H_{\alpha,\gamma}(X)$ as

$$H_{\alpha,\gamma}(X) = \gamma \mathrm{Tr}(X) + \frac{f_\alpha(X)^{\sigma+1}}{X^2}.$$

In the following lemma we collect the properties of f_α and g_β that will be used in the sequel. Most of the properties are straightforward and appeared in [2]. For completeness, we provide a (different) proof here.

Lemma 2.1 *The maps f_α and g_β are both linear on $\mathbf{F}_q$. They also have the following additional properties.*
(i) *For every $x \in \mathbf{F}_q$, we have $\mathrm{Tr}(f_\alpha(x)) = (r + \alpha m)\mathrm{Tr}(x)$ and $f_\alpha(1) = r + \alpha m$.*
(ii) *For every $x \in \mathbf{F}_q$, we have $\mathrm{Tr}(g_\beta(x)) = (k + \beta m)\mathrm{Tr}(x)$ and $g_\beta(1) = k + \beta m$.*
(iii) *For every $x \in \mathbf{F}_q$, we have $f_\alpha(x)^\sigma + f_\alpha(x) = x^2 + x$ and $g_\beta(x)^2 + g_\beta(x) = x^\sigma + x$.*

(iv) *We have that f_α maps $\mathbf{T}_0$ bijectively onto $\mathbf{T}_0$ and maps $\mathbf{T}_1$ bijectively onto $\mathbf{T}_{r+\alpha m}$. In particular, f_α is a permutation on $\mathbf{F}_q$ if and only if $r + \alpha m \equiv 1 \pmod 2$.*
(v) *We have that g_β maps $\mathbf{T}_0$ bijectively onto $\mathbf{T}_0$ and maps $\mathbf{T}_1$ bijectively onto $\mathbf{T}_{k+\beta m}$. In particular, g_β is a permutation on $\mathbf{F}_q$ if and only if $k + \beta m \equiv 1 \pmod 2$.*
(vi) *For every $x \in \mathbf{F}_q$, we have $f_\alpha(g_\beta(x)) = g_\beta(f_\alpha(x)) = x + \delta \mathrm{Tr}(x)$ with*

$$\delta = m' + \alpha k + \beta r + \alpha\beta m.$$

We have that $1 + \delta m = (r + \alpha m)(k + \beta m)$.
(vii) *For every $y \in \mathbf{F}_q$ and for every $\lambda \in \mathbf{F}_2$, we have $g_\beta(y) = g_0(\bar{y}) + \theta \mathrm{Tr}(y)$ with $\bar{y} = y + \lambda \mathrm{Tr}(y)$ and $\theta = \beta + \lambda k$. Here, the element θ of $\mathbf{F}_2$ satisfies $m\theta = k + \beta m + k(1 + \delta m)$.*

Proof: The claims (i) and (ii) are trivial. (Simply note that $\mathrm{Tr}(1) = m$.) The claims in (iii) are easily verified.

Since by (i) f_α is linear, maps $\mathbf{T}_0$ to $\mathbf{T}_0$, and maps $\mathbf{T}_1$ to $\mathbf{T}_{r+\alpha m}$, claim (iv) is equivalent to the claim that if $f_\alpha(x) = 0$ and $\mathrm{Tr}(x) = 0$, then $x = 0$. To show this, suppose that $f_\alpha(x) = 0$. By (iii), we have that $0 = f_\alpha^\sigma(x) + f_\alpha(x) = x^2 + x$, so $x = 0$ or $x = 1$. Now $\mathrm{Tr}(1) = m$ and by (i) we have that $f_\alpha(1) = r + \alpha m$. So $\mathrm{Tr}(1) = 0$ and $f_\alpha(1) = 0$ would imply that $r \equiv m \equiv 0 \bmod 2$, contradicting the assumption that $rk \equiv 1 \bmod m$.

Similarly, claim (v) is equivalent to the claim that if $g_\beta(x) = 0$ and $\mathrm{Tr}(x) = 0$, then $x = 0$, which can be shown in the same way as the claim for f_α above. Indeed, suppose that $g_\beta(x) = 0$. Then by (iii) we have that $0 = g_\beta^2(x) + g_\beta(x) = x^\sigma + x$, and since $\sigma = 2^k$ with $\gcd(k, m) = 1$, we conclude that $x = 0$ or $x = 1$. Again the assumptions that $m = \mathrm{Tr}(1) \equiv 0 \bmod 2$ and $k + \beta m = g_\beta(1) \equiv 0 \bmod 2$ would imply that $m \equiv k \equiv 0 \bmod 2$, which contradicts $rk \equiv 1 \bmod m$.

To prove claim (vi), first note that

$$\begin{aligned} f_0(g_0(x)) = g_0(f_0(x)) &= \sum_{i=0}^{r-1} \sum_{j=0}^{k-1} x^{2^{ki+j}} \\ &= \sum_{t=0}^{kr-1} x^{2^t} \\ &= x^{2^{m'm}} + \sum_{t=0}^{m'm-1} x^{2^t} \\ &= x + m' \mathrm{Tr}(x). \end{aligned}$$

Then use (i), (ii), and the definitions of f_α and g_β to verify claim (vi) for arbitrary α and β. The last part of claim (vi) follows immediately from (i) and (ii) by taking $x = 1$.

Finally, let $\bar{y} = y + \lambda \mathrm{Tr}(y)$. Then

$$\begin{aligned} g_\beta(y) &= \beta \mathrm{Tr}(y) + g_0(y) \\ &= \beta \mathrm{Tr}(y) + g_0(\bar{y} + \lambda \mathrm{Tr}(y)) \\ &= \beta \mathrm{Tr}(y) + k\lambda \mathrm{Tr}(y) + g_0(\bar{y}) \\ &= g_0(\bar{y}) + \theta \mathrm{Tr}(y) \end{aligned}$$

with $\theta = \beta + k\lambda$. To prove the last part of (vii), simply take $y = 1$. This completes the proof of the lemma. □

In what follows, we will show that the polynomial $H_{\alpha,0}(X)$ is closely related to Dickson polynomials. First we observe that in characteristic 2, the Dickson polynomials $D_{2^k-1}(X, 1)$ over $\mathbf{F}_q$ are closely related to the linearized polynomial

$$T_k(X) = X + X^2 + \cdots + X^{2^{k-2}} + X^{2^{k-1}}$$

To simplify notation, we will use $D_n(X)$ to denote $D_n(X, 1)$ over $\mathbf{F}_q$.

Proposition 2.2 *For any $k \geq 1$, $D_{2^k-1}(X) = X^{2^k+1}T_k(1/X)^2$.*

This proposition can be proved by induction, see [1].

We are now ready to relate $H_{\alpha,0}(X) = f_\alpha(X)^{\sigma+1}/X^2$ to $D_{2^k-1}(X)$. We state our result in the following proposition.

Proposition 2.3 *Let m, k, r, m', q, σ be given as in Section 1 with $\gcd(k, m) = 1$. Let $\alpha \in \{0, 1\}$ be such that $r + \alpha m \equiv 1 \pmod 2$, and let $\beta \in \{0, 1\}$ be defined by $\beta \equiv m' + \alpha k \pmod 2$. Then for every $x \in \mathbf{F}_q^*$, we have*

$$H_{\alpha,0}(g_\beta(x)) = x^{\sigma+1}/g_\beta(x)^2 = \begin{cases} 1/D_{2^k-1}(1/x) & \text{if } \beta = 0, \\ 1/D_{2^{m-k}-1}(1/x)^{2^k} & \text{if } \beta = 1. \end{cases}$$

In particular, $H_{\alpha,0}(X)$ is a PP of $\mathbf{F}_q$ if and only if $r + \alpha m \equiv 1 \pmod 2$.

Proof: First note that if $m \equiv 0 \pmod 2$ then $k \equiv 1 \pmod 2$ and $r \equiv 1 \pmod 2$. So it is always possible to choose α such that $r + \alpha m \equiv 1 \pmod 2$. When $r + \alpha m \equiv 1 \pmod 2$, then by Lemma 2.1, part (iv), the linear map f_α is a permutation of $\mathbf{F}_q$. Its inverse is

$$g_\beta(x) = x + x^2 + \cdots + x^{2^{k-1}} + \beta\mathrm{Tr}(x) = T_k(x) + \beta\mathrm{Tr}(x),$$

where β is defined in the statement of the proposition. In particular, we have $k + \beta m \equiv 1 \pmod 2$, by Lemma 2.1, part (v). Therefore for $x \in \mathbf{F}_q^*$ we have

$$H_{\alpha,0}(g_\beta(x)) = f_\alpha(g_\beta(x))^{\sigma+1}/g_\beta(x)^2 = x^{\sigma+1}/g_\beta(x)^2. \tag{2}$$

Case 1. $\beta = 0$. (Hence k is odd.) In this case, $g_\beta(x) = T_k(x)$. Therefore, for every $x \in \mathbf{F}_q^*$, by Proposition 2.2 and (2), we have

$$H_{\alpha,0}(g_\beta(x)) = x^{\sigma+1}/T_k(x)^2 = 1/D_{2^k-1}(1/x). \tag{3}$$

Since $\gcd(k, m) = 1$ and k is odd, we see that $\gcd(2^k - 1, q^2 - 1) = 2^{\gcd(k,2m)} - 1 = 1$. By Theorem 1.1, $D_{2^k-1}(X)$ is a PP of $\mathbf{F}_q$. So (3) implies that $H_{\alpha,0}(X)$ is a PP of $\mathbf{F}_q$.

Case 2. $\beta = 1$. (Hence $k + m \equiv 1 \pmod 2$.) In this case, for $x \in \mathbf{F}_q^*$ (so $g_\beta(x) \neq 0$), we have

$$\begin{aligned} H_{\alpha,0}(g_\beta(x)) &= \frac{x^{2^k+1}}{x^2 + x^{2^2} + \cdots + x^{2^k} + (x + x^2 + \cdots + x^{2^{m-1}})} \\ &= \frac{x^{2^k+1}}{x^{2^k+1} + \cdots + x^{2^m}} \\ &= \left(\frac{x^{2^{m-k}+1}}{x^2 + x^{2^2} + \cdots + x^{2^{m-k}}}\right)^{2^k} \\ &= \left(1/D_{2^{m-k}-1}(1/x)\right)^{2^k} \end{aligned}$$

Since $\gcd(m-k, m) = 1$ and $m - k$ is odd, we see that $\gcd(2^{m-k} - 1, q^2 - 1) = 1$. Hence by Theorem 1.1, $H_{\alpha,0}(X)$ is a PP of $\mathbf{F}_q$.

Finally if $H_{\alpha,0}(X)$ is a PP of $\mathbf{F}_q$, then $r + \alpha m \equiv 1 \pmod 2$ since $H_{\alpha,0}(0) = 0$ and $H_{\alpha,0}(1) = r + \alpha m$.

This completes the proof. □

3 Proof of the Main Theorem

We will need the following lemmas in the proof of our main theorem.

Lemma 3.1 *With the definitions of $H_{\alpha,\gamma}(X)$ and $f_\alpha(X)$ given in Section 1 and 2, for $x \in \mathbf{F}_q^*$, we have*

$$H_{\alpha,\gamma}(x) = \gamma \mathrm{Tr}(x) + \left(\frac{f_\alpha(x)}{x}\right)^2 + \frac{f_\alpha(x)}{x} + f_\alpha(x),$$

and

$$\mathrm{Tr}(H_{\alpha,\gamma}(x)) = (r + (\alpha + \gamma)m)\,\mathrm{Tr}(x).$$

Proof: The first assertion follows from part (iii) of Lemma 2.1. Indeed, for $x \in \mathbf{F}_q^*$, since $f_\alpha(x)^\sigma = f_\alpha(x) + x^2 + x$, we have that $f_\alpha(x)^{\sigma+1} = f_\alpha(x)^2 + f_\alpha(x)(x^2 + x)$. Now

$$\begin{aligned} H_{\alpha,\gamma}(x) &= \gamma \mathrm{Tr}(x) + \frac{f_\alpha(x)^{\sigma+1}}{x^2} \\ &= \gamma \mathrm{Tr}(x) + \left(\frac{f_\alpha(x)}{x}\right)^2 + \frac{f_\alpha(x)}{x} + f_\alpha(x). \end{aligned}$$

The second assertion follows from the first one in combination with part (i) of Lemma 2.1. □

Let m, k, q, σ be as before. Define $\mathbf{B}_0 = (\mathbf{F}_q \setminus \{1\}) \cup \{\infty\}$ and $\mathbf{B}_1 = \{z \in \mathbf{F}_{q^2} \setminus \{0,1\} \mid z^q = z^{-1}\}$. Note that $\mathbf{B}_1 = \{\theta^{(q-1)i} \mid i = 1, \ldots, q\}$, for a primitive element θ of $\mathbf{F}_{q^2}$. Also, define the map ϕ from $\mathbf{F}_{q^2} \cup \{\infty\}$ to itself by

$$\phi(z) = 1/(z + z^{-1}), \tag{4}$$

where the usual convention on the symbol ∞ is adopted (in particular, $\phi(0) = \phi(\infty) = 0$ and $\phi(1) = \infty$). Finally, define the maps w_0 and w_1 from $\mathbf{F}_{q^2} \cup \{\infty\}$ to itself by

$$w_0(z) = z^{\sigma-1}, \qquad w_1(z) = z^{\sigma+1}, \tag{5}$$

for $z \in \mathbf{F}_{q^2}$ and, in addition, $w_e(\infty) = \infty$ for $e = 0, 1$. Our interest in the sets $\mathbf{B}_e$ and the maps ϕ, w_0, and w_1 is explained by the following lemma (see also [3], Lemma 1).

Lemma 3.2 (i) *For $e \in \mathbf{F}_2$, the map ϕ maps $\mathbf{B}_e$ two-to-one onto $\mathbf{T}_e$.*
(ii) *The map w_0 is a permutation of $\mathbf{B}_0$, and it is a permutation of $\mathbf{B}_1$ if and only if $k \equiv 1$ (mod 2).*
(iii) *The map w_1 is a permutation of $\mathbf{B}_0$ if and only if $m \equiv 1$ (mod 2), and a permutation of $\mathbf{B}_1$ if and only if $m + k \equiv 1$ (mod 2).*

Proof: (i). Let $u : \mathbf{F}_{q^2} \cup \{\infty\} \to \mathbf{F}_{q^2} \cup \{\infty\}$ be defined by $u(z) = 1/(z+1)$. Then the map u is one-to-one from $\mathbf{F}_{q^2} \cup \{\infty\}$ to itself, and $\phi(z) = u(z)^2 + u(z)$ for all $z \in \mathbf{F}_{q^2} \cup \{\infty\}$. If $z \in \mathbf{B}_0$, then $u(z) \in \mathbf{F}_q$, hence $\phi(z) \in \mathbf{T}_0$. Since u maps $\mathbf{B}_0$ bijectively to $\mathbf{F}_q$, and the map $z \mapsto z^2 + z$ is two-to-one from $\mathbf{F}_q$ to $\mathbf{T}_0$, we see that ϕ is two-to-one from $\mathbf{B}_0$ to $\mathbf{T}_0$. Now if $z \in \mathbf{B}_1$, then $\phi(z)^q = \phi(z)$, hence $\phi(z) \in \mathbf{F}_q$. But $u(z) \notin \mathbf{F}_q$, so $\phi(z) \in \mathbf{F}_q \setminus \mathbf{T}_0 = \mathbf{T}_1$. One can further verify that u maps $\mathbf{B}_1$ bijectively to the set $\{x \in \mathbf{F}_{q^2} \mid x^q = x+1\}$, which is mapped two-to-one onto $\mathbf{T}_1$ by the map $z \mapsto z^2 + z$. This shows that ϕ is two-to-one from $\mathbf{B}_1$ to $\mathbf{T}_1$.

(ii) and (iii). For any integer s, the map $z \mapsto z^s$ is a permutation of $\mathbf{B}_0$ if and only if $\gcd(s, 2^m - 1) = 1$, and a permutation of $\mathbf{B}_1$ if and only if $\gcd(s, 2^m + 1) = 1$. Now suppose that $\gcd(k, m) = 1$. If $s = 2^k - 1$, then $\gcd(s, 2^m - 1) = 1$ (hence $z \mapsto z^{2^k-1}$ is a permutation of $\mathbf{B}_0$), and $\gcd(s, 2^m + 1) = \gcd(2^k - 1, 2^{2m} - 1)/\gcd(2^k - 1, 2^m - 1) = 2^{\gcd(k,2m)} - 1$. So $\gcd(2^k - 1, 2^m + 1) = 1$ if and only if k is odd. Hence the map $z \mapsto z^{2^k-1}$ is a permutation of $\mathbf{B}_1$ if and only if $k \equiv 1 \bmod 2$. Next, if $s = 2^k + 1$, then $\gcd(s, 2^m - 1) = \gcd(2^k + 1, 2^m - 1) = \gcd(2^{2k} - 1, 2^m - 1)/\gcd(2^k - 1, 2^m - 1) = 2^{\gcd(m,2k)} - 1$. So $\gcd(2^k + 1, 2^m - 1) = 1$ if and only if m is odd. Finally

$$\begin{aligned} \gcd(2^m + 1, s) &= \gcd(2^m + 1, 2^k + 1) \\ &= \gcd(2^{2m} - 1, 2^k + 1)/\gcd(2^m - 1, 2^k + 1) \\ &= (2^{\gcd(2m,2k)} - 1)(2^{\gcd(m,k)} - 1)/((2^{\gcd(m,2k)} - 1)(2^{\gcd(2m,k)} - 1)), \end{aligned}$$

so $\gcd(2^m + 1, 2^k + 1) = 1$ if and only if precisely one of k, m is odd. □

In the sequel we will use the map ϕ defined in (4) and the maps w_0 and w_1 defined in (5) to simplify an equation involving $g_\beta(x)$, $x \in \mathbf{F}_{q^2}$, using the following lemma.

Lemma 3.3 *Let m, k, q, σ be defined as in Section 1.*
(i) *For $z \in \mathbf{F}_{q^2} \setminus \{0, 1\}$, we have that*

$$\sum_{j=1}^{k} (z + z^{-1})^{-2^j} = (z^{\sigma-1} + z^{1-\sigma})/(z + z^{-1})^{\sigma+1}.$$

(ii) *For $z \in \mathbf{F}_{q^2} \setminus \{0, 1\}$, we have that $g_0^2(\phi(z)) = (\phi(z))^{\sigma+1}/\phi(w_0(z))$ and $1 + g_0^2(\phi(z)) = (\phi(z))^{\sigma+1}/\phi(w_1(z))$.*

Proof: To prove (i), we use induction on k. For $k = 1$, we have $\sigma = 2$ and the assertion is trivial. Next, if the assertion holds for k, then using induction hypothesis, we have for $z \in \mathbf{F}_{q^2} \setminus \{0, 1\}$

$$\begin{aligned}
\sum_{j=1}^{k+1} (z + z^{-1})^{-2^j} &= (z^{\sigma-1} + z^{1-\sigma})/(z + z^{-1})^{\sigma+1} + (z + z^{-1})^{-2\sigma} \\
&= \Big((z^{\sigma-1} + z^{1-\sigma})(z + z^{-1})^{\sigma} + (z + z^{-1})\Big)/(z + z^{-1})^{2\sigma+1} \\
&= (z^{2\sigma-1} + z^{1-2\sigma})/(z + z^{-1})^{2\sigma+1},
\end{aligned}$$

and the assertion holds also for $k + 1$. This proves (i).

The first assertion in (ii) is a direct consequence of (i); the second assertion is a consequence of the fact that $(z + z^{-1})^{\sigma+1} = z^{\sigma+1} + z^{\sigma-1} + z^{-\sigma+1} + z^{-\sigma-1}$. □

We are now ready to give the proof of our main theorem.

Proof of Theorem 1.2. By Lemma 3.1, the mapping $H_{\alpha,\gamma} : x \mapsto H_{\alpha,\gamma}(x)$, $x \in \mathbf{F}_q$, maps $\mathbf{T}_0$ to $\mathbf{T}_0$, and maps $\mathbf{T}_1$ to $\mathbf{T}_{r+(\alpha+\gamma)m}$. So it suffices to show that $H_{\alpha,\gamma}$ is injective on both $\mathbf{T}_0$ and $\mathbf{T}_1$. For $x \in \mathbf{T}_0$, we have $H_{\alpha,\gamma}(x) = H_{0,0}(x) = H_{1,0}(x)$. Since $\gcd(m, r) = 1$, it is always possible to choose $\alpha \in \{0, 1\}$ such that $r + \alpha m \equiv 1 \pmod 2$. It follows from Proposition 2.3 that $H_{\alpha,\gamma}$ maps $\mathbf{T}_0$ to $\mathbf{T}_0$ bijectively.

Now we show that if

$$H_{\alpha,\gamma}(x) = H_{\alpha,\gamma}(y), \text{ and } x, y \in \mathbf{T}_1, \tag{6}$$

then $x = y$. Simplifying (6), we get

$$\frac{f_\alpha(x)^{\sigma+1}}{x^2} = \frac{f_\alpha(y)^{\sigma+1}}{y^2}. \tag{7}$$

Since $\gcd(m, k) = 1$, it is possible to choose $\beta \in \{0, 1\}$ such that $k + \beta m \equiv 1 \pmod 2$. By Lemma 2.1, part (v), g_β maps $\mathbf{T}_1$ bijectively to $\mathbf{T}_{k+\beta m} = \mathbf{T}_1$. Let a, b be elements of $\mathbf{T}_1$ such that $g_\beta(a) = x$ and $g_\beta(b) = y$. Substituting x, y in (7) by $g_\beta(a)$ and $g_\beta(b)$ respectively, and applying Lemma 2.1, part (vi), we have

$$\frac{(a + \delta)^{\sigma+1}}{g_\beta(a)^2} = \frac{(b + \delta)^{\sigma+1}}{g_\beta(b)^2}, \tag{8}$$

where $\delta \equiv m' + \alpha + \beta r \pmod 2$. Set $a + \delta = \bar{a}$ and $b + \delta = \bar{b}$. Applying Lemma 2.1, part (vii), with $\lambda = \delta$, we have

$$\frac{\bar{a}^{\sigma+1}}{g_0(\bar{a})^2 + \theta} = \frac{\bar{b}^{\sigma+1}}{g_0(\bar{b})^2 + \theta}, \tag{9}$$

where $\theta \equiv \beta + \delta k \pmod 2$. Note that since $k + \beta m \equiv 1 \pmod 2$, we have

$$m\theta \equiv 1 + k(1 + \delta m) \pmod 2 \tag{10}$$

If one of $\bar{a}, \bar{b}$ is zero, then by (9), the other one is also zero, hence $a = b$, and therefore $x = y$. So from now on we assume that $\bar{a} \neq 0$ and $\bar{b} \neq 0$. Then we obtain from (9) that

$$\frac{g_0(\bar{a})^2}{\bar{a}^{\sigma+1}} + \frac{\theta}{\bar{a}^{\sigma+1}} = \frac{g_0(\bar{b})^2}{\bar{b}^{\sigma+1}} + \frac{\theta}{\bar{b}^{\sigma+1}}. \tag{11}$$

Note that $\mathrm{Tr}(\bar{a}) = \mathrm{Tr}(\bar{b}) = 1 + \delta m$, hence by Lemma 3.2, part (i), we have $s, t \in \mathbf{B}_{1+\delta m}$ $(s, t \neq 0, 1, \infty)$ such that

$$\bar{a} = \phi(s) = \frac{1}{s + s^{-1}} \text{ and } \bar{b} = \phi(t) = \frac{1}{t + t^{-1}},$$

where the map ϕ is defined before the statement of Lemma 3.2. Plugging these into (11) and applying Lemma 3.3, part (ii), we have

$$s^{\sigma-1} + s^{1-\sigma} + \theta(s + s^{-1})^{\sigma+1} = t^{\sigma-1} + t^{1-\sigma} + \theta(t + t^{-1})^{\sigma+1},$$

that is,

$$\phi(w_\theta(s)) = \phi(w_\theta(t)),$$

where w_θ, $\theta \equiv 0$ or $1 \pmod 2$, is defined before the statement of Lemma 3.2.

By Lemma 3.2, part (i), since the map ϕ is two-to-one from $\mathbf{B}_e$ to $\mathbf{T}_e$ ($e = 0$ or 1), we have $w_\theta(s) = w_\theta(t)$ or $w_\theta(s) = w_\theta(t)^{-1} = w_\theta(t^{-1})$. By (10), if $\theta = 0$ and $1 + \delta m \equiv 1 \pmod 2$, then $k \equiv 1 \pmod 2$; also, if $\theta = 1$, then $1 + \delta m \equiv 0 \pmod 2$ implies that $m \equiv 1 \pmod 2$, and $1 + \delta m \equiv 1 \pmod 2$ implies that $m \equiv 1 + k \pmod 2$. So by Lemma 3.2, part (ii) and (iii), the map $z \mapsto w_\theta(z)$ is a permutation of $\mathbf{B}_{1+\delta m}$. Therefore we have either $s = t$ or $s = t^{-1}$, both lead to $\bar{a} = \bar{b}$, hence $a = b$, therefore $x = y$. This completes the proof. □

Remark 1. In the above proof that $H_{\alpha,\gamma}$ is injective on $\mathbf{T}_e$ for $e = 0$ and $e = 1$, different proofs were given for the two cases. However, it is not difficult to adapt the above proof given for the case $e = 1$ so that it works for both cases $e = 0$ and $e = 1$. To this end, we first define the translation maps τ_v for $v = 0, 1$ by $\tau_v(x) = x + v$. Now choose β such that $k + \beta m \equiv 1 \pmod 2$ (this is possible since k and m are relatively prime), define δ as in Lemma 2.1, part (vi), and let $\theta \in \{0, 1\}$ satisfy $\theta \equiv \beta + \delta k \pmod 2$, so that (10) holds. Let $e \in \{0, 1\}$. We will in fact show that for all z in $\mathbf{B}_{e(1+\delta m)}$,

$$H_{\alpha,\gamma}(g_\beta(\tau_{\delta e}(\phi(z))) = \tau_{\gamma e}(\phi(w_{\theta e}(z))). \tag{12}$$

To see this, let $z \in \mathbf{B}_{e(1+\delta m)}$. Now observe that $\bar{y} := \phi(z) \in \mathbf{T}_{e(1+\delta m)}$ by Lemma 3.2, part (i). So $y := \bar{y} + \delta e = \tau_{\delta e}(\bar{y}) \in \mathbf{T}_e$, and by Lemma 2.1, part (ii), we have $x := g_\beta(y) \in \mathbf{T}_e$. Furthermore, as a consequence of our choices for β, δ, and θ, we have by Lemma 3.2, part (vi), that $f_\alpha(g_\beta(y)) = \bar{y}$, and by Lemma 3.2, part (vii) with $\lambda = \delta$, that $g_\beta(y) = \theta e + g_0(\bar{y})$. Also, if $z \notin \{0, \infty\}$, we can conclude from Lemma 3.3 that $\theta e + g_0^2(\phi(z)) = \phi(z)^{\sigma+1}/\phi(w_{\theta e}(z))$, and it is easily verified that this equation also holds when $z \in \{0, \infty\}$. Using these observations, we conclude that

$$\begin{aligned} H_{\alpha,\gamma}(x) &= H_{\alpha,\gamma}(g_\beta(y)) \\ &= \gamma e + f_\alpha(g_\beta(y))^{\sigma+1}/g_\beta^2(y) \\ &= \gamma e + \bar{y}^{\sigma+1}/(\theta e + g_0^2(\bar{y})) \\ &= \gamma e + \phi(z)^{\sigma+1}/\Big(\phi(z)^{\sigma+1}/\phi(w_{\theta e}(z))\Big) \\ &= \gamma e + \phi(w_{\theta e}(z)), \end{aligned}$$

that is, (12) holds.

Now by Lemma 3.2, part (ii) and (iii) and by (10), the map $w_{\theta e}$ is a permutation on $\mathbf{B}_{e(1+\delta m)}$. Moreover, by Lemma 3.2, part (i), ϕ maps $\mathbf{B}_{e(1+\delta m)}$ two-to-one onto $\mathbf{T}_{e(1+\delta m)} = \mathbf{T}_{e(r+\alpha m)}$ (see Lemma 2.1, part (vi)), and this set is in turn mapped one-to-one onto $\mathbf{T}_{e(r+(\alpha+\gamma)m)}$ by the map $\tau_{\gamma e}$. So the composition map $z \mapsto \tau_{\gamma e}(\phi(w_{\theta e}(z)))$ in the right-hand side of (12) is two-to-one from $\mathbf{B}_{e(1+\delta m)}$ onto $\mathbf{T}_{e(r+(\alpha+\gamma)m)}$. On the other hand, ϕ maps $\mathbf{B}_{e(1+\delta m)}$ two-to-one onto $\mathbf{T}_{e(1+\delta m)}$, the map $\tau_{\delta e}$ maps this set one-to-one onto $\mathbf{T}_e$, and g_β is a permutation on $\mathbf{T}_e$, so the composition map $z \mapsto H_{\alpha,\gamma}(g_\beta(\tau_{\delta e}(\phi(z))))$ is two-to-one if and only if $H_{\alpha,\gamma}$ is one-to-one on $\mathbf{T}_e$. Combining these two observations, we conclude that $H_{\alpha,\gamma}$ is one-to-one on $\mathbf{T}_e$ for both $e = 0$ and $e = 1$.

Remark 2. In the case where $\gamma = 1$ and m is odd, if $r + (\alpha + \gamma)m \equiv 1 \pmod 2$, then $r + \alpha m \equiv 0 \pmod 2$, hence by Theorem 1.2, $H_{\alpha,0}(X)$ is not a PP of $\mathbf{F}_q$. Yet, by adding $\mathrm{Tr}(X)$ to $H_{\alpha,0}(X)$, we see that $H_{\alpha,1}(X) = \mathrm{Tr}(X) + H_{\alpha,0}(X)$ is a PP of $\mathbf{F}_q$.

Remark 3. When $k = 1$ (so $\sigma = 2$ and $r = 1$), the map $H_{1,1} : \mathbf{F}_q \to \mathbf{F}_q$ fixes $\mathbf{T}_0$ elementwise and maps $x \in \mathbf{T}_1$ to $x + 1/x + 1/x^2$. Therefore, by Theorem 1.2 the map $h : \mathbf{T}_1 \to \mathbf{T}_1$ defined by $h(x) = x + 1/x + 1/x^2$ is a permutation of $\mathbf{T}_1$. This fact was used in [5] to prove a Kloosterman sum identity.

Remark 4. We give one more example to illustrate Theorem 1.2. Let k, m be positive integer such that $2k \equiv 1 \pmod m$. Let $\sigma = 2^k$. Then $\sigma^2 \equiv 2 \pmod{2^m - 1}$. In this case, we have $r = 2$, and

$$H_{0,0}(X) = X^{\sigma-1} + X^{2(\sigma-1)} + X^{\sigma^2-1} + X^{\sigma^2+\sigma-2},$$

and

$$H_{0,1}(X) = \mathrm{Tr}(X) + X^{\sigma-1} + X^{2(\sigma-1)} + X^{\sigma^2-1} + X^{\sigma^2+\sigma-2}.$$

By Theorem 1.2, $H_{0,0}$ maps $\mathbf{T}_0$ bijectively to $\mathbf{T}_0$, and $\mathbf{T}_1$ bijectively to $\mathbf{T}_0$; and $H_{0,1}$ maps $\mathbf{T}_0$ bijectively to $\mathbf{T}_0$, and $\mathbf{T}_1$ bijectively to $\mathbf{T}_1$. In particular, $H_{0,1}(X)$, and hence also the

polynomial

$$\mathrm{Tr}(X) + X^{\sigma-1} + X^{2(\sigma-1)} + X + X^{\sigma}$$

are PPs of $\mathbf{F}_q$

Acknowledgement: The research of the second author was partially supported by NSA grant MDA 904-03-1-0095. The authors thank an anonymous referee for his/her careful reading of the paper.

References

[1] S. D. Cohen, R. W. Matthews, *Exceptional polynomials over finite fields*, Finite Fields Appl. **1** (1995), 261–277.

[2] H. Dobbertin, *Kasami power functions, permutation polynomials and cyclic difference sets*, Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), 133–158, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542, Kluwer Acad. Publ., Dordrecht, 1999.

[3] G. L. Ebert, S. Egner, H. D. L. Hollmann, Q. Xiang, *Proof of a conjecture of DeCaen and van Dam*, Europ. J. Combinatorics, **23** (2002), 201–206.

[4] H. D. L. Hollmann, Q. Xiang, *Pseudocyclic association schemes arising from the action of* $\mathrm{PGL}(2, 2^m)$ *and* $\mathrm{P\Gamma L}(2, 2^m)$, submitted.

[5] H. D. L. Hollmann, Q. Xiang, *Kloosterman sum identities over* $\mathbf{F}_{2^m}$, Discrete Math. **279** (2004), 277–286.

[6] R. Lidl, H. Niederreiter, Finite Fields, second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997

[7] R. Lidl, G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly, **95** (1988), 243–246.

[8] R. Lidl, G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field? II*, Amer. Math. Monthly, **100** (1993), 71–74.

[9] R. Lidl, G. L. Mullen, and G. Turnwald, Dickson polynomials. Pitman Monographs and Surveys in Pure and Applied Mathematics, 65. Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

[10] W. Nöbauer, *Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen* (German), J. Reine Angew. Math. **231** (1968), 216–219

[11] G. L. Mullen, *Permutation polynomials over finite fields*, Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991), 131–151, Lecture Notes in Pure and Appl. Math., 141, Dekker, New York, 1993.